Audit and Management Advisory Services
Computer Environment Internal Control Questionnaire

Date:

Completed By:

Name:
Department:
Position:
Phone:
Email Address:

Section 1: Security Education and Awareness Training

1. What types of ongoing network administration training do you receive?

2. Have you attended any Campus Security training or seminars?

3. Is the administrator subscribed to the sysadmin-l and Security-Discuss-L list?

Section 2: Asset Inventory & Classification

1. How many departmental servers do you manage? What are their functions? (Mail, File/Print, Web, etc.) and their OS.

2. How many workstations do you manage? What type of operating system do they run?

3. Do you support Laptops, Tablets, PDA's, Blackberry, SmartPhone, Routers/Switches, etc? If so, how many?

4. Do you regularly perform an inventory of hardware? If so, how often and when was the last inventory completed?

5. Do you maintain any other network documentation? (If so, please provide any Spreadsheets, Visio or other Network Maps, etc.)

Section 3: Risk Assessment

1. Has the department performed a risk assessment to determine the characteristics of the information/data stored on or transmitted from/to departmental computing devices? If so, when was the last risk assessment performed?

2. Critical data, that becomes unavailable for any reason, could have an adverse effect on department operations. Describe the type of files or data that are critical to the operation of the department.

3.What type of sensitive data (if any) is stored on devices in your department? (FERPA, HIPAA, PII, PCI, PI)

Section 4: Information Security Plan

1. Has a plan been developed that takes into consideration the acceptable level of risk for systems and processes?

2. Have additional departmental policies, procedures or standards been established for general security control? If yes, what areas do they cover? (Please provide a copy)

Section 5: Workforce Administration

1. Please identify your primary and backup network administrators as well as any other IT support personnel (DB Administrators, Web Administrators, External IT Support, etc.)

2. What procedures are in place for employee terminations or job changes to ensure user access is removed or adjusted?

Section 6: Physical Security / Environmental Controls

1. Are servers, routers, switches, firewalls, wiring closets, etc. physically restricted to authorized personnel? If so, what restrictions are in place.

2. Do you maintain current lists of persons with access to such hardware? If so, when was it last updated? Please provide the list as an attachment.

3. Have there been any physical security compromises in the last year? What were the results of the incidents?

4. Is cabling secured to limit exposure to accidental or intentional disconnection or disturbance?

5. What environmental controls are in place to protect equipment from heat, fire or water damage?

6. Are servers connected to a UPS? If so, how long can the UPS support the servers and are they configured to support controlled shutdown or continued processing?

7. What procedures are in place for the physical security of mobile devices? (laptops, PDA's. etc)

8. Are users educated on the responsibilities of mobile device ownership including risks to data and mitigation steps to reduce that risk? How is this documented. (provide documentation if any)

Section 7: Incident Response Planning and Notification Procedures

1. Is a monitoring process implemented to log, detect and respond to unusual events related to security? (e.g., excessive failed attempts to authenticate) If so, please describe.

2. Is an automated monitoring tool used to track incidents and alert administrators? If so please describe.

3. What do you do in the event of a security incident?

4. What procedures are in place to respond to and manage infected systems? (Response Team, if any, and its members, removing system from network, etc.)

Section 8: Third Party Agreements

1. Who is responsible for approving budgeted hardware and software acquisitions?

2. Are your equipment purchases submitted through the Campus Purchasing Dept.? If not, how do you assure yourself that vendor support and system security features are addressed in purchase agreements?

Section 9: Identity and Access Management

1. Are you running your own authentication store (Active Directory (AD), Kerberos, Local Users) or are you using campus AD?

2. Do you develop web applications that require authentication in your department?

a. If yes, are you using the campus SSO(Single Sign On)?
b. If not SSO, what are you using?

3. Do you use privileged or administrative accounts only for administrative purposes and a separate account for other daily activities?

4. Does each administrator have a unique admin account or do administrators share a common account?

5. Are users educated about guidelines to establish secure passwords?

6. Are new users forced to enter a new password on initial login?

7. Are there minimum and maximum password length requirements?

8. Are default passwords used?

9. Is password complexity enforced? (uppercase, lowercase, numeric, special characters, etc.)

10. Is password expiration enforced? If yes, how often are users required to change password?

11. Is password history maintained? If yes, how many are remembered to prevent reuse?

12. Are account lockout settings in place? If yes, please elaborate on number of failures before lockout, duration of lockout and/or method to reset account.

13. Are there additional password controls in place? If so, please describe.

14. Are users discouraged from using "Remember Password" features? If so, how are passwords managed?

15. Are you using any encrypted authentication mechanisms? (ssh, sftp, scp, ftps, etc)

Section 10: Access Controls to Authenticate & Authorize Users

1. What is the process to manage access requests?

2. Are standardized roles or group based security templates used to help manage specific user access rights? If so, please elaborate.

3. How long can a user remain idle in their session before they are locked out?

4. Are "guest" or "visitor" accounts used to access the network? If so, please explain the circumstances under which "guest" or "visitor" accounts are used.

5. Are group or shared IDs/Passwords allowed? If so, please explain who uses them and what they are used to access.

Section 11: Application Systems Management

1. Are you running or developing any in-house applications, web or otherwise? If so, please describe.

2. Is there any original or custom source code on any of the servers you support?

3. Do you currently have software development and/or quality assurance environments?

4. Do any of the applications developed in-house support the storage, transmission or processing of sensitive personal or restricted information? If so, please describe.

5. Are your websites compliant with ADA requirements (Americans with Disabilities Act)?

6. Is a formal software change control process in place?

7. Who has access to the production environment?

8. Who can migrate changes to production environment?

9. Is there a segregation of duties between programmers and users with access to migrate changes into production?

Section 12: Collection, Management and Analysis of Log Data

1. How is security activity monitored? Describe what, if any, activity is logged and the process to review it. (audit trails)

2. What is the process to act on any adverse conditions when indicated by log data?

3. What type of log data is configured and maintained?

Section 13: Data Protection and Encryption

1. Is encryption used on departmental servers or workstations? If so, please describe.

2. What are the encryption key management practices?

3. What process is in place for servicing or decommissioning devices?

4. What process is in place to prevent consistent storage of files and data on workstations?

5. How often are web history and caches cleared?

6. Is there a process to identify unencrypted data residing on workstations?

Section 14: Risk Mitigation Measures

1. What procedures are in place to recover servers and resume processing in the event of a system failure?

2. What, if any, server redundancy has been built? (Clusters, Doubletake, etc.)

3. Have system recovery procedures been tested? If so, when was the last test and what were the results?

Section 15: Network Security Tools and Practices

1. Are workstations and servers registered with ACT? Is stored PHI identified as part of the registration?

2. What, if any, anti-virus software is utilized on all servers, workstations, etc.?

3a. What procedures are in place to ensure that anti-virus software and anti-virus definitions are kept current for both servers and workstations?

3b. What procedure is in place to ensure that devices do not contain viruses?

4. What procedure is in place to ensure that workstations and servers receive timely software updates?

5. What procedures are in place to ensure only necessary services are enabled on systems? Are there periodic reviews of system services?

6. Is the network divided into separate security segments? If so, please elaborate.

7. Are firewalls implemented as part of the security architecture?

8. If firewalls are implemented, please elaborate on types (Host based/Hardware/Both), who administers firewalls, firewall log file review process, etc.

9. What criteria are used to manage and configure the firewall(s)?

10. Please describe, at a high level, the process to maintain awareness of, obtain and implement available system patches, fixes and updates (automated, manual, schedule, native to OS or third party, etc.)

Thank You For Completing the Survey